

Computerlinks University 2005!

18-Ottobre.2005

ISS: proiettata nel futuro. L'azienda e la sua visione del Mercato.

Stop Internet threats **before impact** with **preemptive** security from Internet Security Systems

Michele Di Pierro

Alliance&Partner Manager

Internet Security Systems

Mail: mdipierro@iss.net

Mobile: +39-348-2664577



 **INTERNET | SECURITY | SYSTEMS®**

Agenda

- Who is ISS
- Security: The Market
- Security: The Problem
- Security: The ISS Solution.

Agenda

■ Who is ISS

- Security: The Market
- Security: The Problem
- Security: The ISS Solution.

ISS Mission

***To be the premier provider of
enterprise protection solutions and
our customer's trusted security
provider.***

ISS Company Background

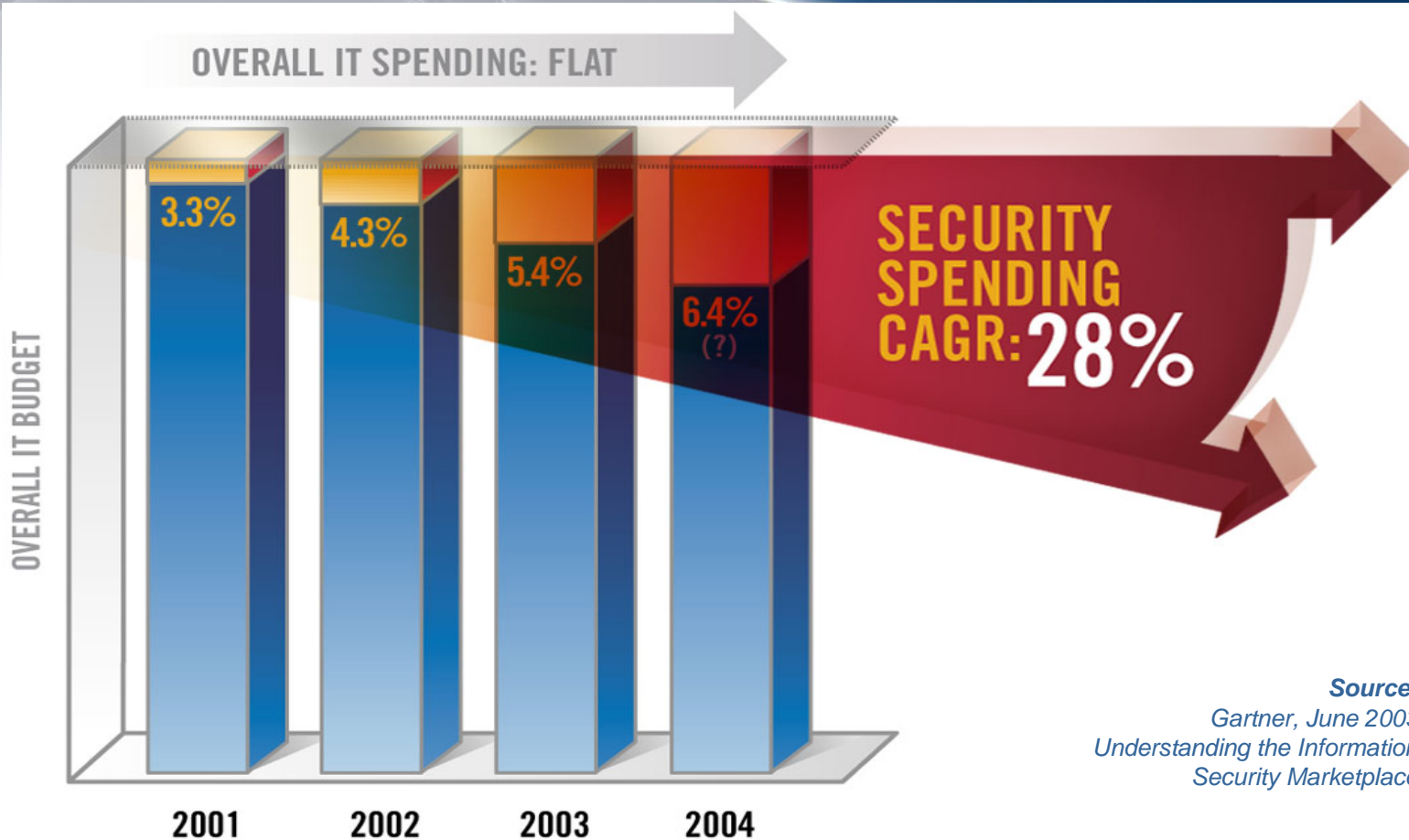
- **World's leading independent IT security provider**
- **Founded in 1994**
- **Headquartered in Atlanta**
- **1998 IPO – NASDAQ: ISSX**
- **1,200 employees in 25 countries**
- **Pioneer and world leader in intrusion prevention**
- **Pioneer and world leader in vulnerability assessment**
- **2004 revenues ~ \$290 million**
- **Profitable, no debt, \$238 million in cash and marketable securities**



Agenda

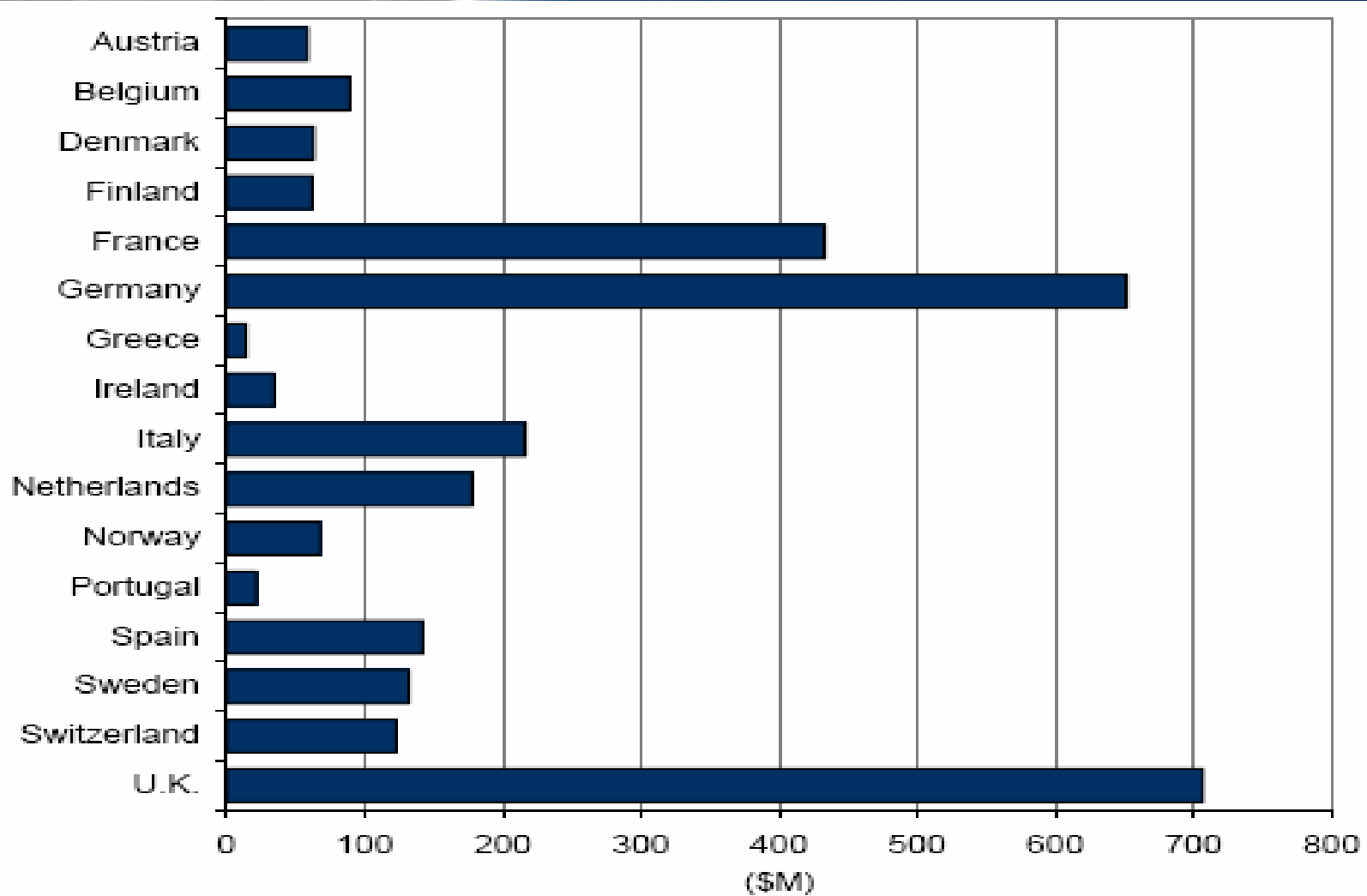
- Who is ISS
- Security: The Market
- Security: The Problem
- Security: The ISS Solution.

Security Spending is Eating Into the IT Budget



Source:
Gartner, June 2003
Understanding the Information
Security Marketplace

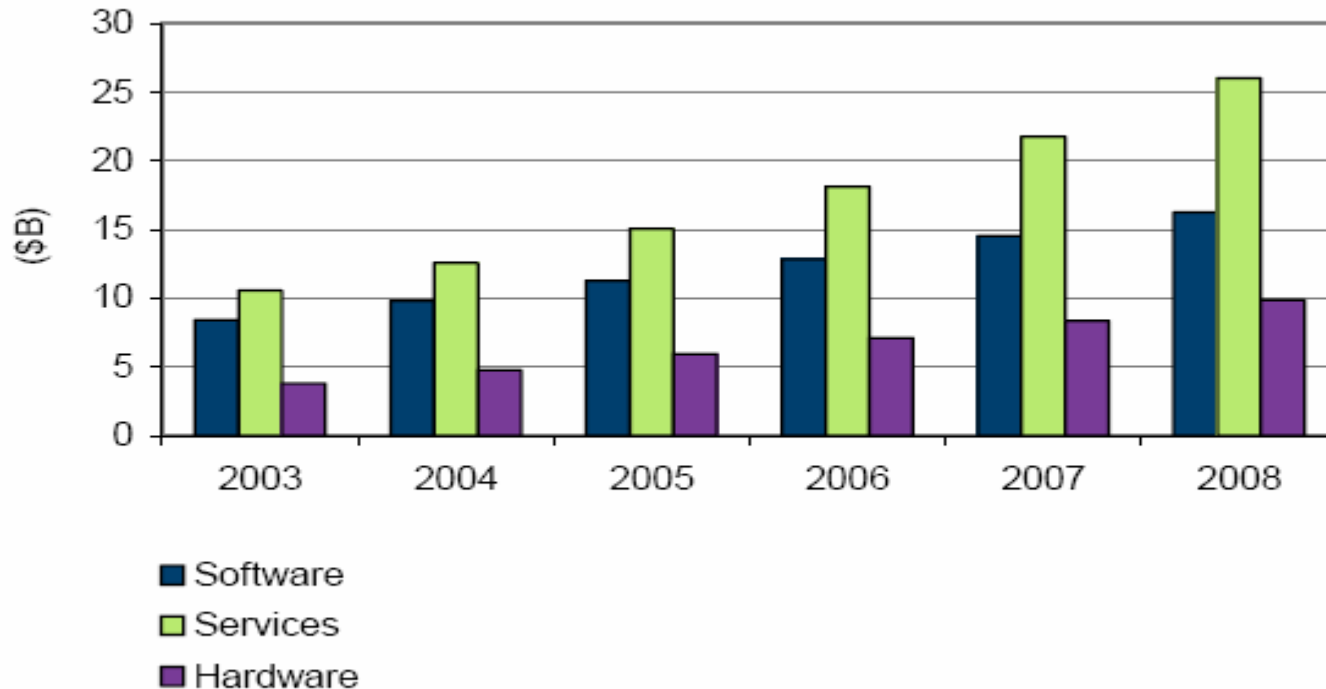
EMEA Countries 2004



Source: IDC, 2005

IDC Forecasts and Assumptions

Worldwide IT Security Revenue by Market, 2002–2008

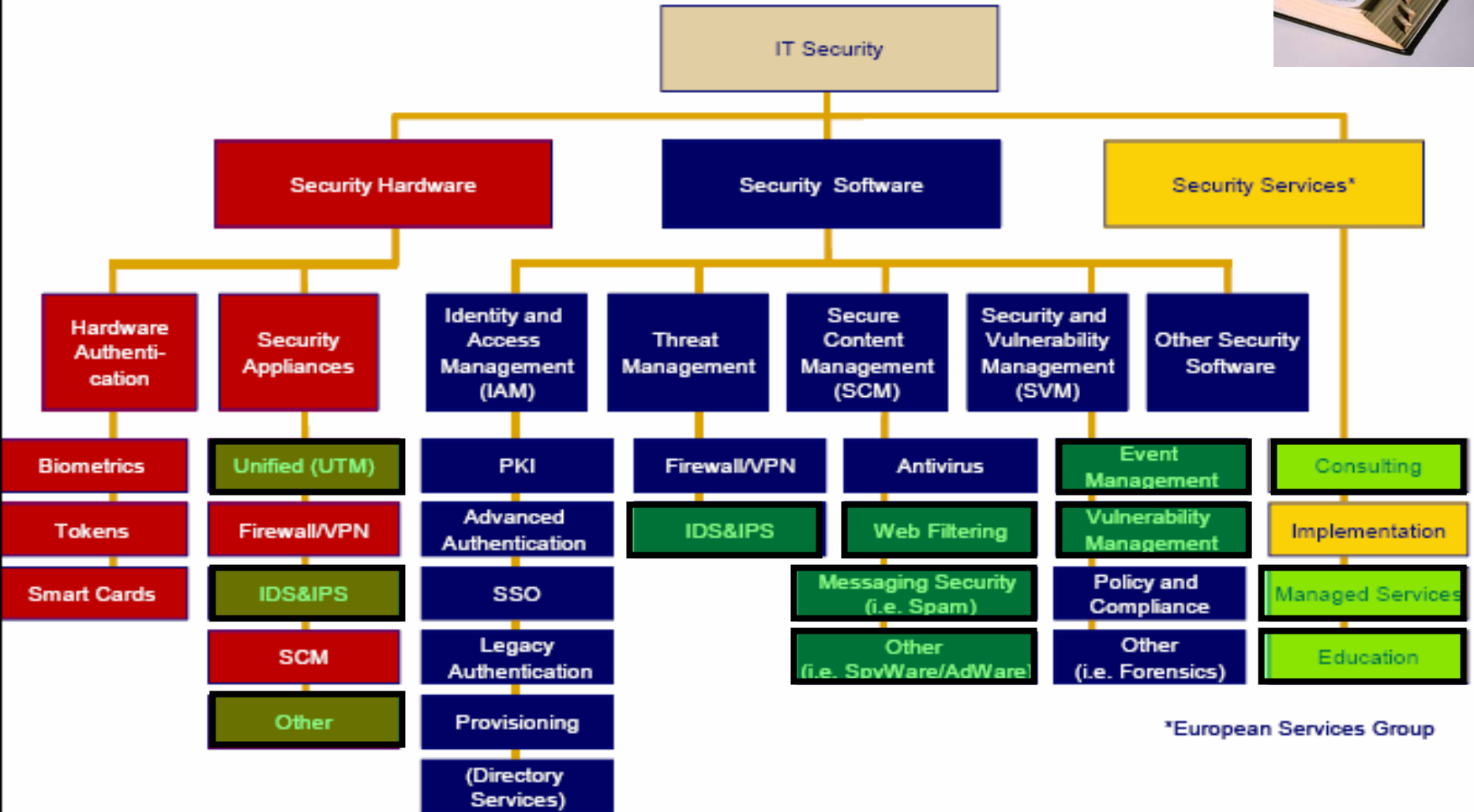


Source: IDC, 2004

The total IT security market achieved a level of \$22.8 billion in 2003, representing 19% growth over 2002. IDC currently forecasts this market to reach \$52.2 billion in 2008, representing a compound annual growth rate (CAGR) of 18% (see Figure).

Security Market Segmentation : Software, Hardware and Services

IDC Security Taxonomy, 2005



*European Services Group

Source: IDC, 2005

The ISS Market Opportunity

<u>Product/Service</u>	<u>2004</u>	<u>2005</u>	<u>2006</u>	<u>2007</u>	<u>CAGR</u>
Vuln Assessment	\$516.0	\$603.8	\$694.3	\$784.6	15.0%
Network IDS/IPS appliances	\$356.6	\$499.3	\$624.1	\$717.7	26.3%
Server IDS/IPS	\$248.5	\$285.7	\$312.4	\$332.8	10.2%
Corp Personal FW	\$163.7	\$230.8	\$301.6	\$369.8	31.2%
URL Filtering	\$421	\$522	\$645	\$786	23.1%
Anti-spam	\$593	\$829	\$1,087	\$1,380	32.5%
UTM (Proventia M)	\$225.0	\$517.5	\$828.0	\$1,324.8	80.6%
Security Services (MSS/PSS)	\$12,210	\$14,488	\$17,284	\$20,591	19.0%
Total	\$14,733.8	\$17,976.1	\$21,776.4	\$26,286.7	21.3%

Agenda

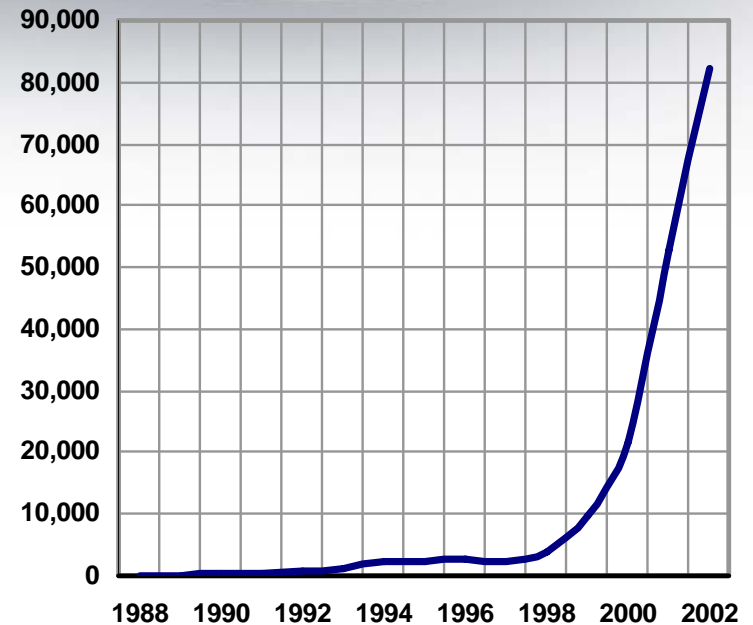
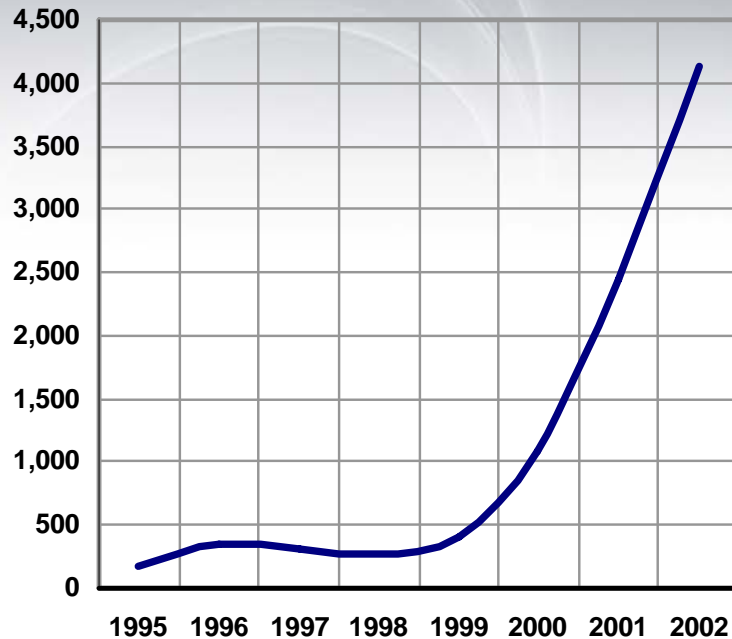
- Who is ISS
- Security: The Market
- Security: The Problem
- Security: The ISS Solution.

*E' questo il corretto approccio
alla security?*

“.....non succedera' a me.”



Vulnerabilities and Incidents Accelerate



DDoS | Viruses | Worms | Trojans | Malicious Code | Exploits | Buffer Overflow | Unauth. Access | Misuse

Threat Spectrum

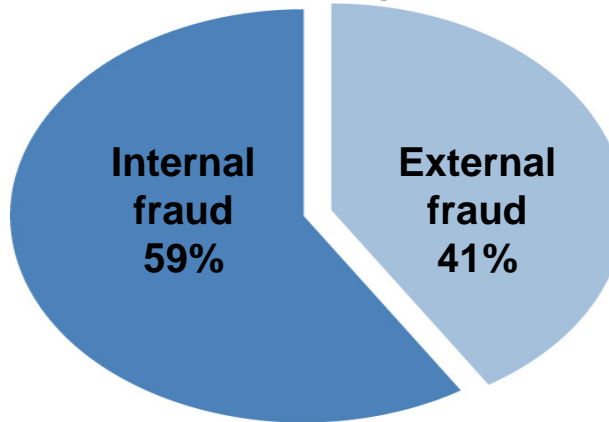
Source: Carnegie Mellon Software Engineering Institute – CERT Coordination Center

Cosa c'e' in gioco?



Corporate
Remote Users
VPN

Frodi commesse dall'INTERNO ed ESTERNO in Europa



European Economic Crime Survey 2001
PriceWaterhouseCoopers

ne

Reactive Patching Can't Keep Up

“It is a never-ending cycle, trying to keep up with this stuff”

- Toyota



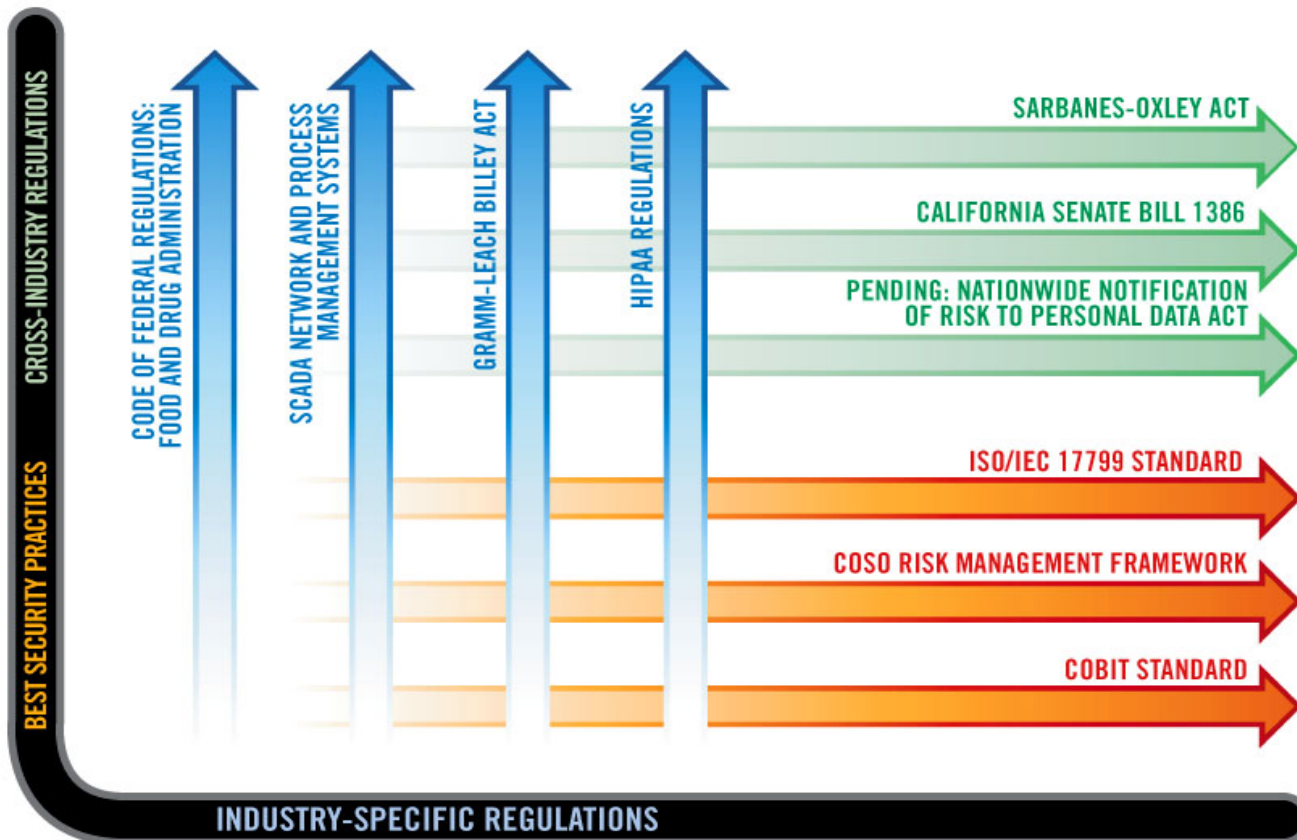
“It takes 30-60 days to install a single patch at every one of our 110 bases”

- US Air Force



Source: Forbes, May 26, 2003

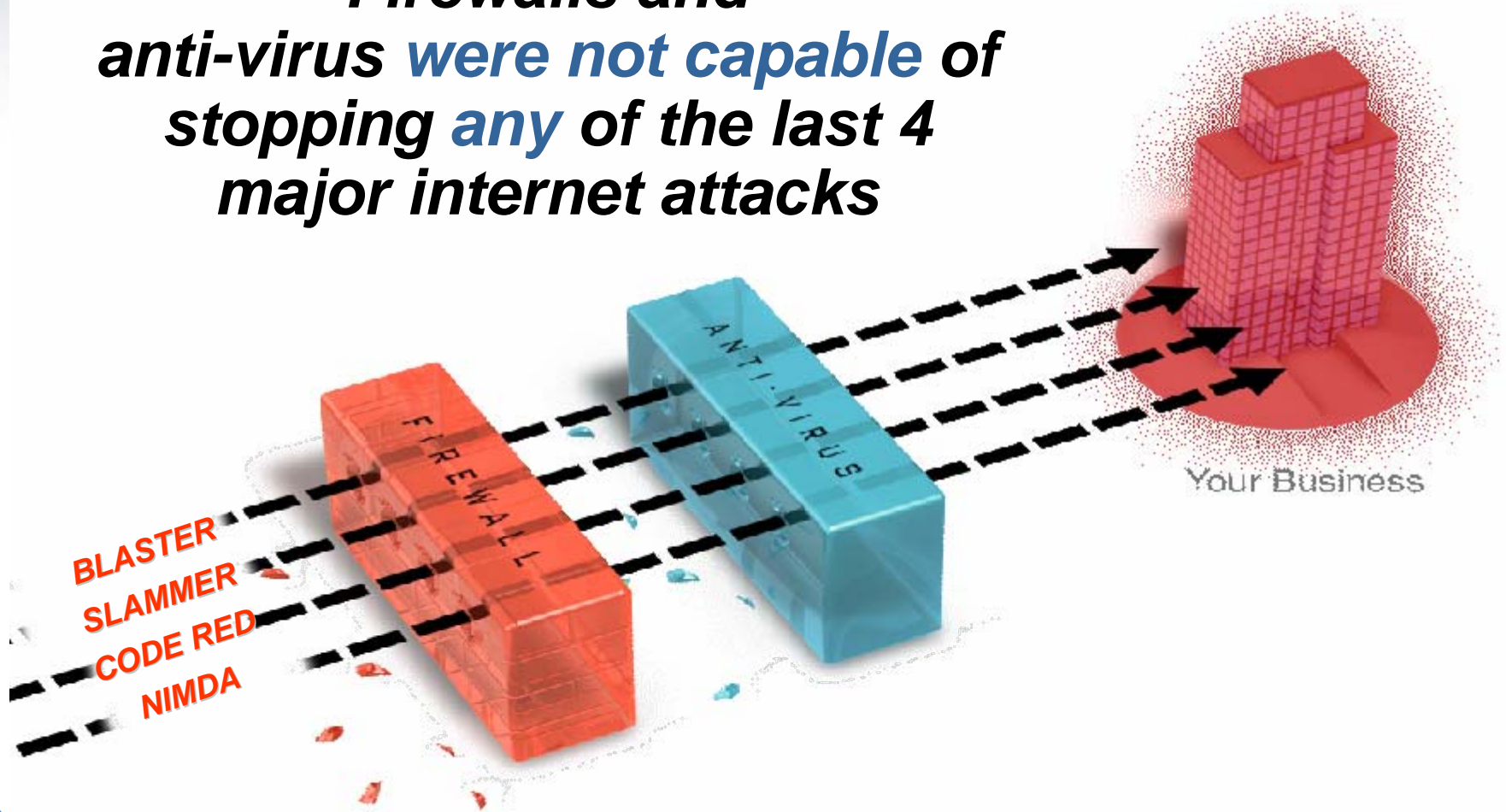
Reactive security does not help regulatory compliance



Can you demonstrate **security due diligence** through separation of duties, written policies and checks & balances?

***And With All This Complexity,
You Still Aren't Protected!***

***Firewalls and
anti-virus were not capable of
stopping any of the last 4
major internet attacks***

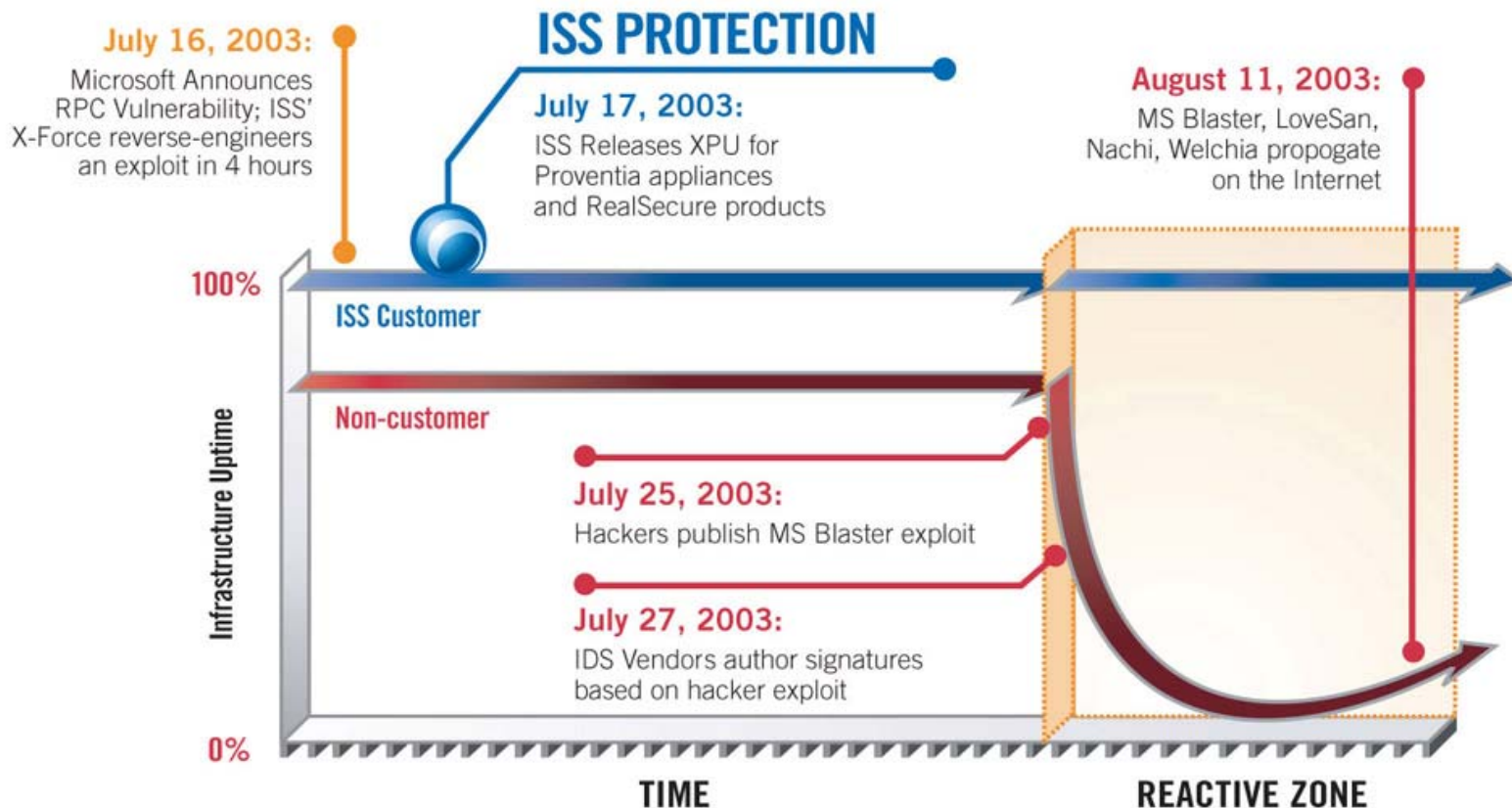


Agenda

- Who is ISS
- Security: The Market
- Security: The Problem
- Security: The ISS Solution.

Reactive security can't protect your business - you need Preemptive Protection

Internet threats spread so rapidly that no "reaction" is fast enough



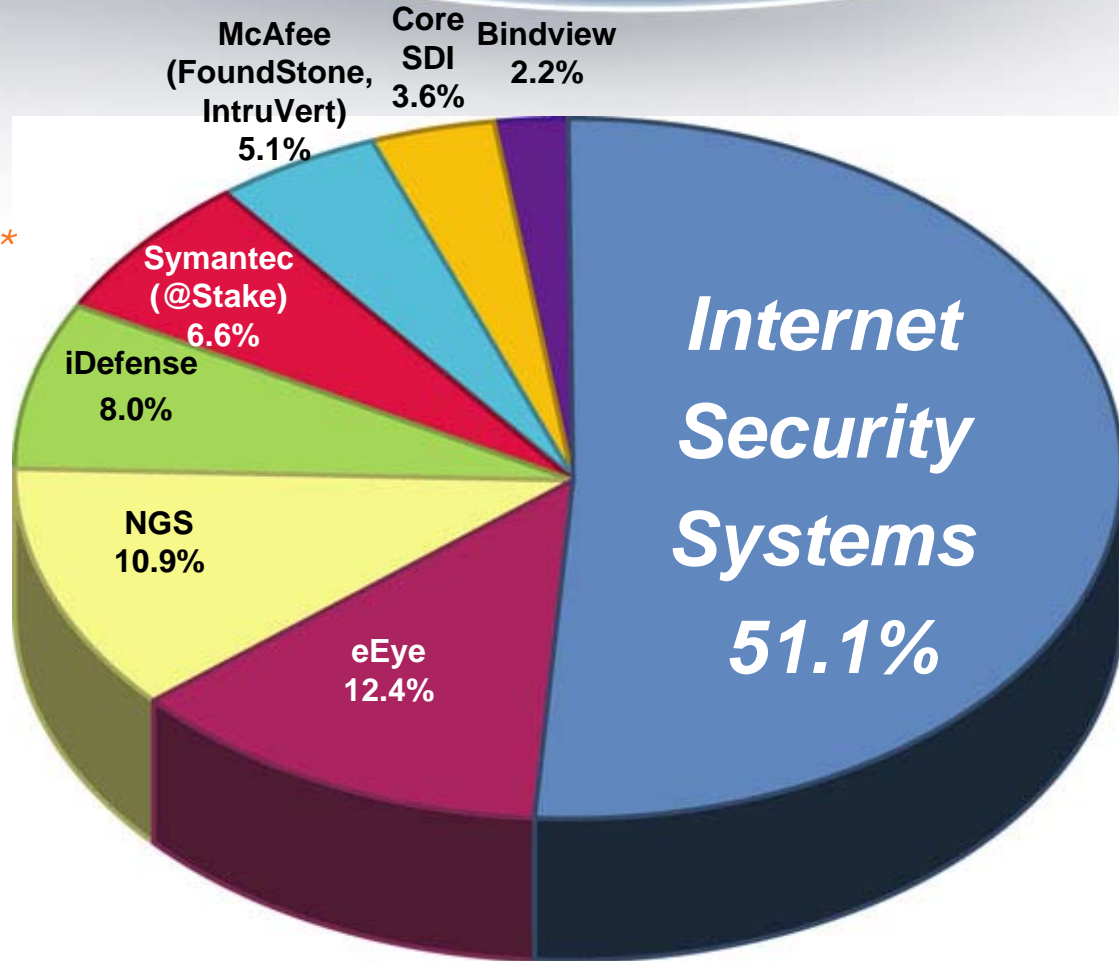
Unique R&D team : X-Force

- **The foundation of ISS' preemptive approach to Internet security is its X Force® research and development team.**
- **ISS can stop more threats because it knows more – by discovering, researching and testing software vulnerabilities and collaborating with government agencies, industry consortiums and software developers.**
- **With this powerful combination, ISS creates effective defenses before attacks ever occur. ISS' knowledge-based approach to protection is extended across the Proventia Enterprise Platform**
- **More information : <http://xforce.iss.net/>**



ISS X-Force: Core Differentiator

High Risk Vulnerabilities 1998-2005**



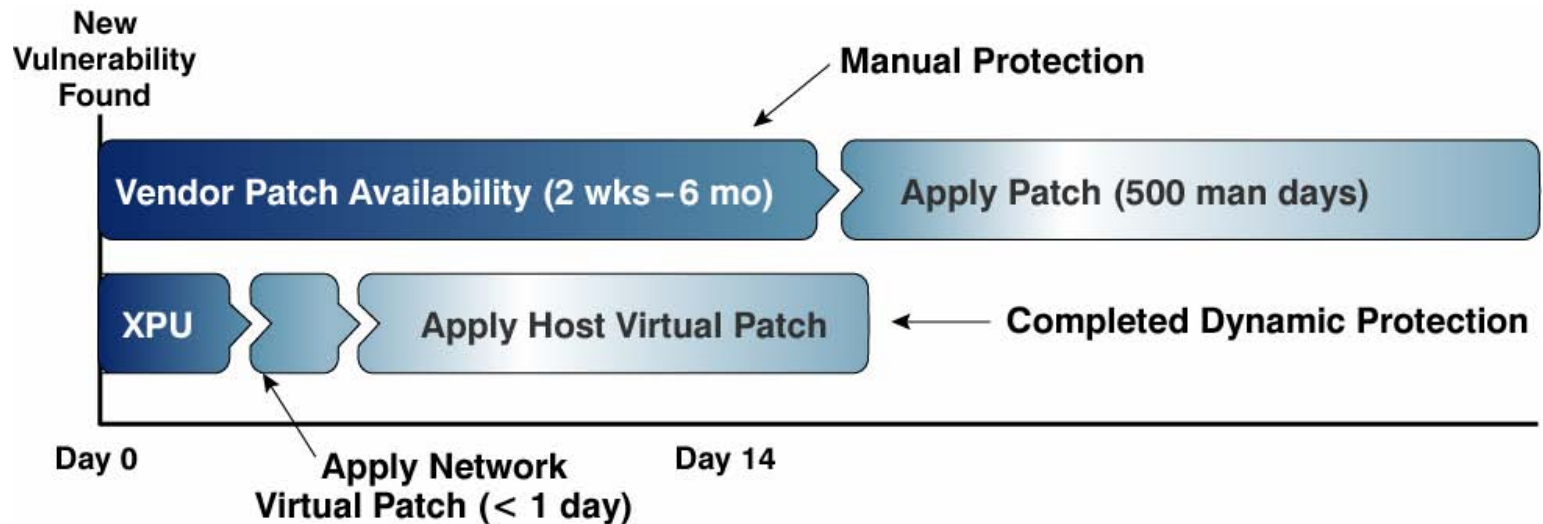
- * High risk vulnerabilities are comprised meet the following combination of conditions:
- lead to remote compromise (compromise over a network)
 - do not require user interaction to exploit
 - do not require authentication to exploit

** As of Q1 2005

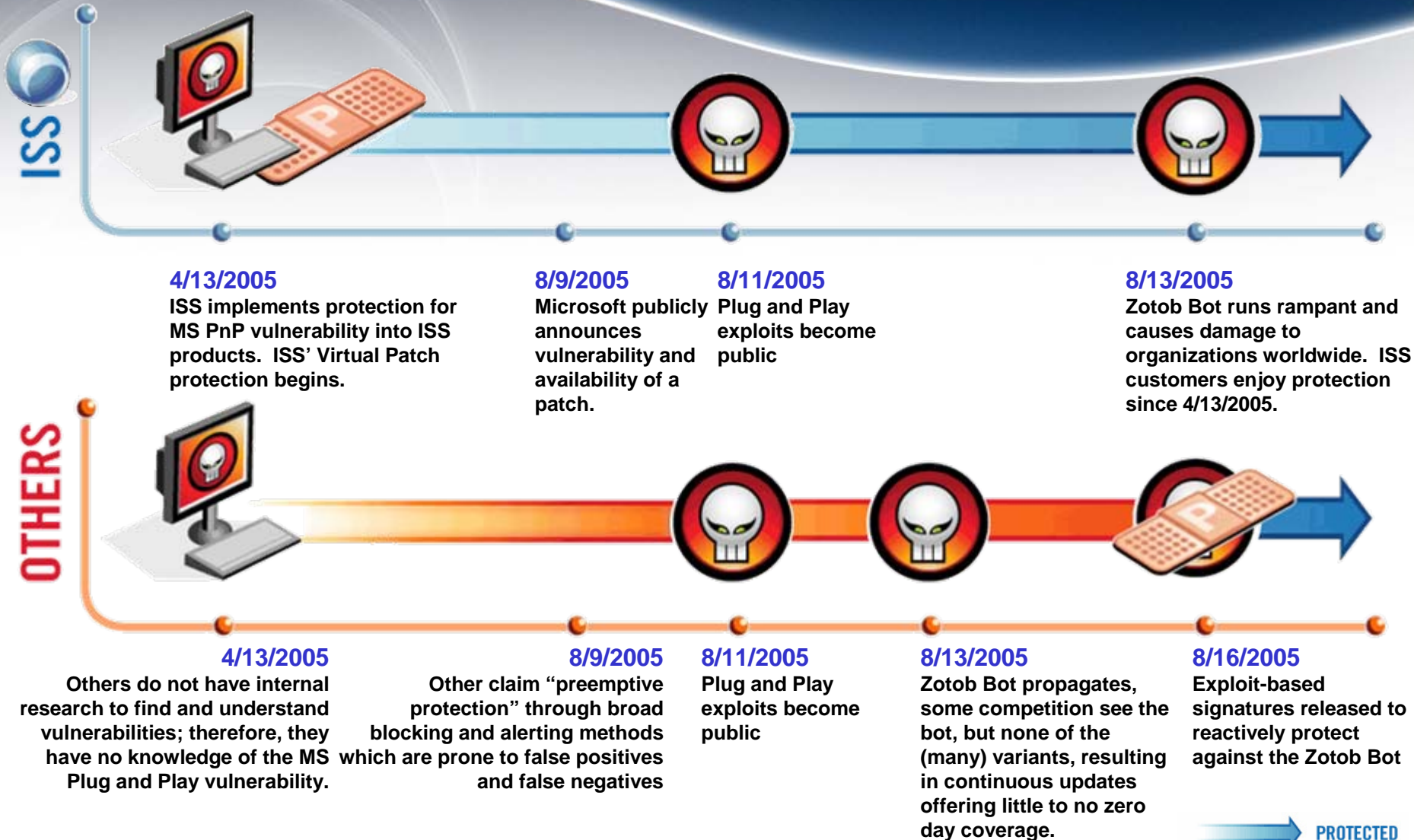
Source: Frost & Sullivan, April 2005

Virtual Patch™: Dynamic Threat Protection

Dynamic threat protection provides a buffer of time via the virtual patch whereby newly discovered exposures are addressed before scheduled patches and upgrades can be applied.



MS Plug and Play / Zotob Timeline



proventia

Enterprise Security Platform (ESP)
is The **Key** to Preemptive Protection



How we deliver Preemptive Protection

The Proventia[®] Enterprise Security Platform enables a four-step process to continuously understand:

1. What is at risk
Vulnerability Mapping

2. What to protect first
Protection prioritization



4. How to show return on investment (ROI)
Reporting and Benchmarking

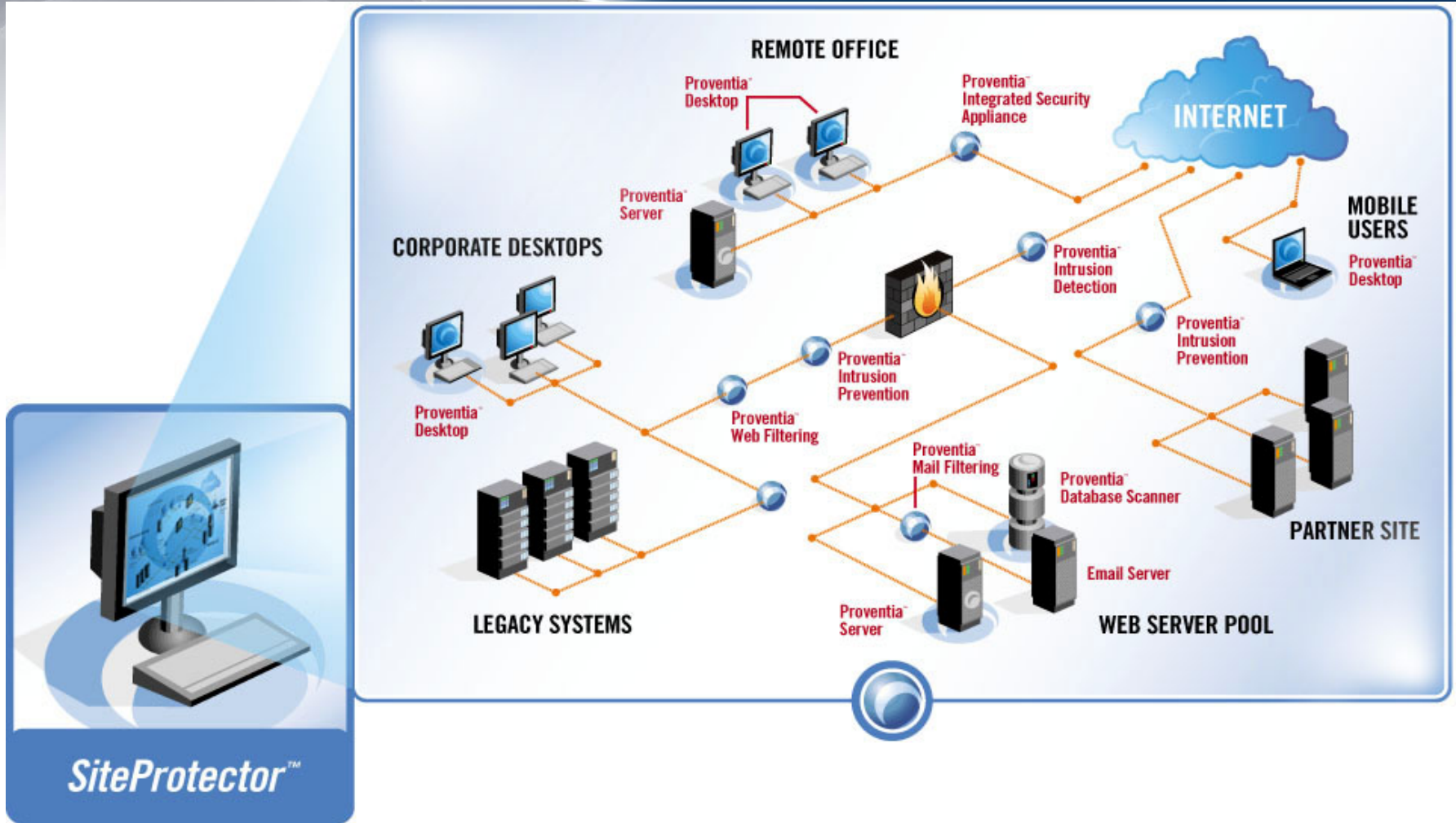
3. How to protect the entire IT infrastructure
Threat prevention and shielding

Proventia ESP – Product & Service View

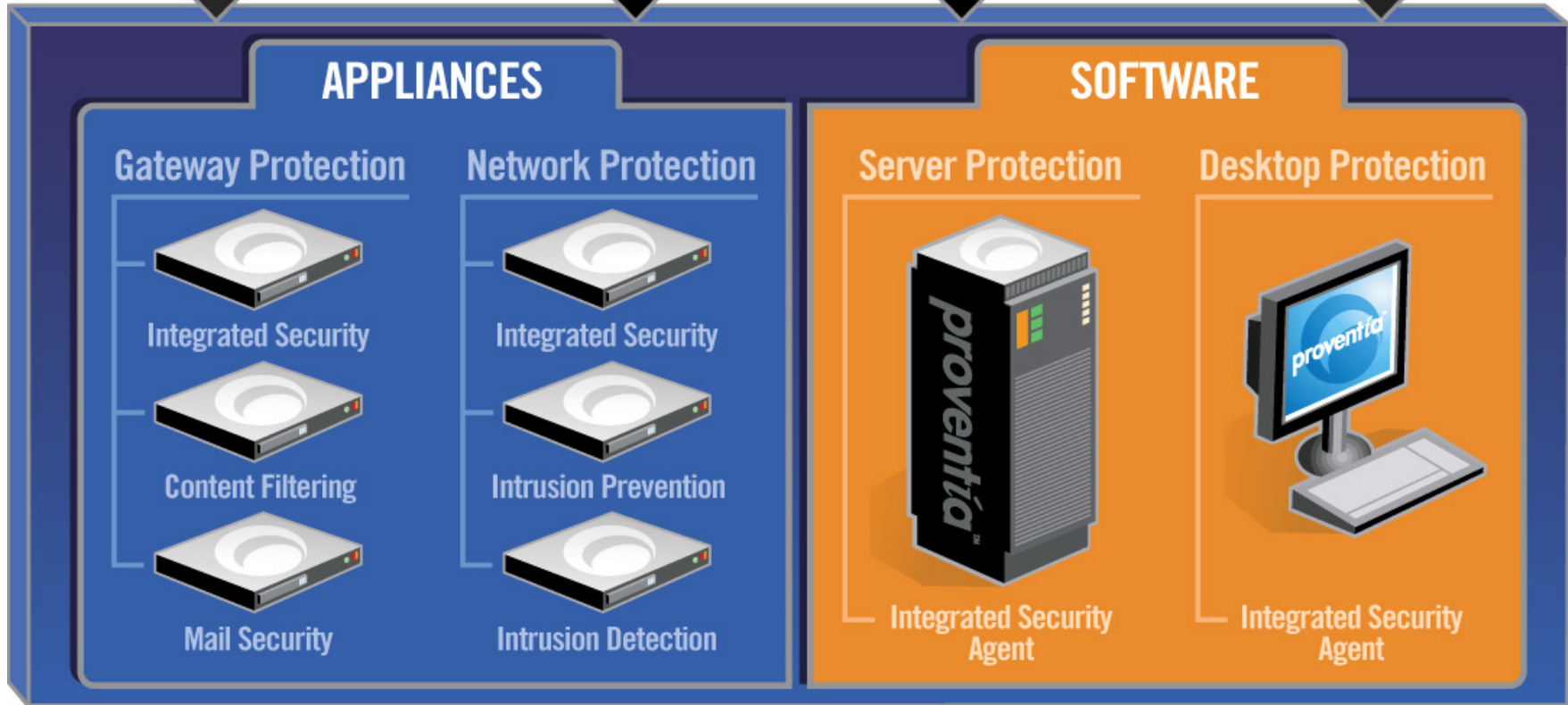
The Proventia® Enterprise Security Platform (ESP) – a Product/Service View



Unified Central Management: SiteProtector



SiteProtector **proventia™** *SiteProtector*



*Virus Prevention System &
Buffer Overflow Exploit Prevention
Preemptive Protection Technology*

Buffer Overflow Exploit Prevention (BOEP)

- A signature-less technology that actively looks for malicious code exploits in memory buffer overflows.
- It stops worms from propagating and prevents attackers from using buffer overflows to run arbitrary code on your systems

VPS is a pre-execution malware analysis technology

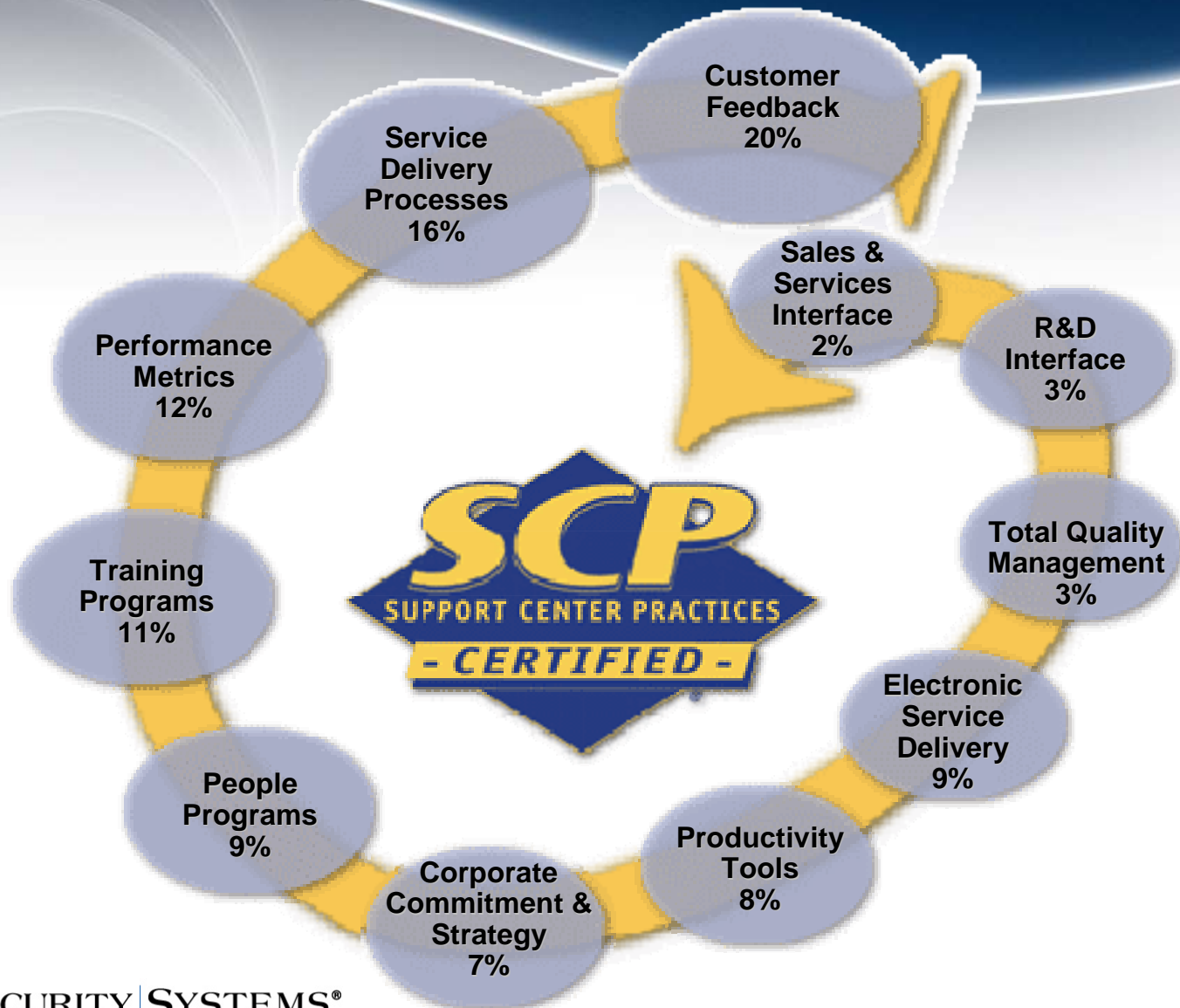
- An **innovative new technology** for signature-free malware prevention.
- Reduces security exposure by preemptively blocking unknown viruses, worms and malware using behavioral-based analysis techniques rather than traditional signatures.

ISS – The leading Independent IT Security Solutions Provider

Trusted by the most demanding security customers in the world...

- 17 of the **world's largest banks**
- 15 of the Largest **Governments around the world** *Based on GNI*
- 11 of the **world's largest public insurance companies**
- 13 of the **world's largest IT companies**

Customer Support Services



Thank You

Michele Di Pierro
Alliance&Partner Manager
Internet Security Systems
Mail: mdipierro@iss.net
Mobile: +39-348-2664577



 **INTERNET | SECURITY | SYSTEMS®**